

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MINNESOTA

GOVERNOR JESSE VENTURA, a/k/a)
James G. Janos, individually,)
)
Plaintiff,)
)
v.) Civil Action No. 11-cv-00174
) SRN-AJB
)
JANET NAPOLITANO,)
Secretary of the Department of)
Homeland Security, et al.,)
)
Defendants.)

I, Lee R. Kair, do hereby declare as follows:

Relevant Experience

1. I am the Assistant Administrator for Security Operations (Assistant Administrator) for the Transportation Security Administration (TSA) within the Department of Homeland Security (DHS). I have held this position since October 2008.

2. As Assistant Administrator, I am responsible for providing executive management of daily field operations for a workforce of approximately 48,000 employees at more than 450 airports nationwide.

3. As Assistant Administrator, my responsibilities include:

- (1) Managing TSA's domestic security operations (with the exception of law enforcement), including the security operations and administrative procedures for all commercial airports, and the management

of all Transportation Security Officers (TSOs), inspectors, and other resources;

- (2) Overseeing compliance by transportation industry entities with a broad range of statutory, regulatory, and program security requirements through inspection of operations and facilities;
- (3) Providing the capacity to detect, deter, and assess explosives threats to the transportation infrastructure, and providing key technical resources to all TSA elements for crisis response and consequence management, including conducting explosives threat analyses, providing support to Federal Air Marshal Service (FAMS) teams and aircraft in flight, and testing and evaluating explosives-related issues;
- (4) Serving as the senior TSA manager and the primary point of coordination for transportation security in all modes (except maritime transportation);
- (5) Enforcing TSA's transportation security related regulations, orders, and requirements;
- (6) Authoring and coordinating security procedures and training documents, Security Directives, Emergency Amendments, orders, and security programs;
- (7) Approving and amending Airport Security Program(s) (ASP) and ensuring that the ASP complies with the applicable guidance and national policy regarding the Federal Security Director's role and authority for day-to-day airport security incidents, coordination of air piracy security responses, law enforcement responses to security incidents in coordination with FAMS' Special Agents in Charge, and transportation security planning;
- (8) Managing all aspects of the TSO workforce;
- (9) Coordinating security initiatives for all transportation modes, including planning and executing aviation and other modal surge activities and pilot security programs;

- (10) Conducting crisis action planning and management for national security special events; and
- (11) Ensuring that private screening officers maintain the standards for safety and security established for TSOs.

4. Prior to becoming Assistant Administrator, I was the Federal Security Director (FSD) for TSA at the Orlando International Airport in Orlando, Florida, which included oversight responsibility for security at the Orlando International Airport and Orlando Sanford International Airport. As FSD, one of my main responsibilities was the implementation of transportation security for passengers and all individuals entering the sterile area of the airport, aircraft, airports and other transportation facilities at those airports. Additionally, I was responsible for developing and monitoring ASPs for the airports under my oversight, as well as coordinating TSA's involvement in Visible Intermodal Protection and Response (VIPR) operations involving TSOs, Federal Air Marshals, airport law enforcement, police, TSA's bomb appraisal officers, and canine teams.

5. I have held several other positions within TSA, including Executive Director of the Office of Intra-Agency Operations. This office operated the TSA "War Room" that tackled strategic issues for TSA, which included TSA's detection of improvised explosive devices (IEDs), redesigning the

passenger screening process, partnerships with stakeholders in other modes of transportation, and increasing the retention, utilization and effectiveness of the TSA workforce.

6. Due to the nature of my official duties, I am familiar with TSA's aviation security program, including the use of Advanced Imaging Technology (AIT) and pat-down procedures to screen passengers before allowing them to proceed into the sterile area of any airport in the United States providing commercial passenger service, as defined in 49 C.F.R. § 1540.5. The statements made in this declaration are based on my personal knowledge, information made available to me in the performance of my official duties, and conclusions reached in accordance therewith.

TSA's Mission

7. Following the events of September 11, 2001, it was clear that the security screening at airports was not sufficient to protect the traveling public. In response, Congress created TSA in order to better secure all modes of transportation, including aviation. At that time, pursuant to congressional mandate, TSA was charged with screening all passengers before they could board an aircraft, as set forth in 49 U.S.C. §§ 44901, 44902, and 44903.

8. It is TSA's mission to prevent terrorist attacks and reduce the vulnerability of the United States to terrorism

within the nation's transportation networks. In meeting its mission, TSA's goal at all times is to maximize transportation protection and security and minimize passenger inconvenience and invasiveness in response to ever-evolving terrorist threats.

TSA's Standard Operating Procedures

9. The Administrator of TSA, John Pistole, is responsible for approving TSA's Standard Operating Procedures (SOPs). As indicated above, as Assistant Administrator, I am responsible for developing, authoring and implementing - and in some cases approving - TSA's SOPs, including those with regard to AIT and the revised pat-down procedures.

10. TSA issues SOPs that apply to specific aspects of the security screening process, and which set forth the uniform procedures and standards that must be followed in TSA's security operations in order to enforce its mandate of providing aviation security. The Screening Checkpoint SOP sets forth in detail the mandatory procedures that TSOs must apply in screening passengers at all airport checkpoints, and which passengers must follow in order to enter the sterile area of any airport.¹ This SOP establishes uniform procedures and standards to screen individuals and accessible property in order to deter, detect,

¹The SOP is not attached to this declaration because it constitutes Sensitive Security Information, pursuant to 49 U.S.C. § 114(r) and controlled under 49 CFR parts 15 and 1520, and cannot be publicly released.

and prevent the carriage of any explosive, incendiary, or weapon (referred to as prohibited items) into a sterile area or onboard an aircraft.

11. On September 17, 2010, TSA issued a newly revised Screening Checkpoint SOP (with an implementation date of October 29, 2010), which included the most recently updated procedures for detecting nonmetallic explosive devices and weapons. This SOP was approved by the Administrator of TSA, and it represents TSA's final agency decision directing the use of AIT machines as part of TSA's standard security screening procedures, as well as the use of revised procedures for the standard pat-down. TSA considers the SOP to be a "final order" pursuant to 49 U.S.C. § 46110.

12. The SOP has since been revised to incorporate changes to the screening procedures for pilots.² The SOP is revised as necessary - and often upon short notice - to account for necessary changes to security procedures in response to terrorist threats, threat assessments, and/or intelligence. For example, in 2004 the SOP was changed to include revised pat-down protocols that increased the frequency and thoroughness of pat-downs, particularly with respect to the breast area, after terrorists destroyed two domestic Russian passenger aircraft in-

²These revisions have no effect on the procedures for screening passengers at airport checkpoints implemented on October 29, 2010.

flight using explosives that were concealed on two female passengers. Likewise, in 2006 the SOP was changed to include the ban on liquids in carry-on luggage following the liquid explosives terrorist plot regarding flights originating in the United Kingdom. Each time the SOP is revised, it is only after TSA has made a final determination that the change to the standard procedures is necessary to ensure a uniform procedure, and to further TSA's mission to maximize transportation protection and security and minimize passenger inconvenience and invasiveness in response to ever-evolving terrorist threats.

AIT

13. TSA began testing and evaluating AIT in 2007, and in 2009 Congress appropriated funds under the American Recovery and Reinvestment Act (ARRA), Pub. L. 111-5, in order to accelerate deployment of such technology to detect weapons and explosives on passengers. In keeping with Congress's directive to TSA in 49 U.S.C. § 44925 to evaluate and deploy advanced screening technology, TSA engaged in extensive laboratory and operational testing of two AIT systems.

14. On January 7, 2010, following the bombing attempt on December 25, 2009, the President issued a "Presidential Memorandum Regarding 12/25/2009 Attempted Terrorist Attack," which charged TSA with aggressively pursuing enhanced screening technology in order to prevent further such attempts, while at

the same time protecting passenger privacy. A copy of that memorandum can be found at <http://www.whitehouse.gov/the-press-office/presidential-memorandum-regarding-12252009-attempted-terrorist-attack>.

15. Based on the latest intelligence and an assessment of the available technologies, TSA determined that using AIT as a primary screening device was the most effective technology available to detect threat items concealed on airline passengers, such as the non-metallic explosives used by Umar Farouk Abdulmutallab in his attempt to blow up an American passenger airliner. The decision to use AIT as a primary screening method is reflected in TSA's Screening Checkpoint SOP, described above.

16. TSA has approved two AIT systems for operational use. One of those systems is the Rapiscan Secure 1000, also known as a backscatter x-ray. The reason the Rapiscan Secure 1000 is referred to as "backscatter" x-ray is because the machine creates an image using very small amounts of x-ray that are bounced back off of the person being screened to sensitive detectors in the machine. These reflected x-rays are then processed by computer to form an image that will show anomalies hidden under a passenger's clothing.

17. The other AIT system in use is the L-3 ProVision, which uses millimeter-length radio waves to achieve the same

result as the backscatter x-ray. Millimeter wave technology bounces harmless electromagnetic waves off of the human body to detectors in the machine, which a computer then interprets in order to create a black and white image.

18. These machines are the very latest in technological advancement and may eventually replace walk-through metal detectors, which have been in place since the 1960s. However, at present, AIT machines have not replaced walk-through metal detectors, and no security checkpoint uses only AIT screening technology. Rather, the AIT machines are used as part of TSA's multi-layered security procedures, and passengers are screened either by AIT or by walk-through metal detector.

19. AIT machines have not been deployed to all airports. As of January 2011, TSA has deployed 486 AIT machines to 78 airports nationwide. TSA's goal is to deploy nearly 1,000 AIT machines by the end of calendar year 2011. A continually updated list of airports where AIT is deployed can be found on TSA's website at <http://www.tsa.gov/approach/tech/ait/faqs.shtm>. The ability to deploy AIT to airports and the number of machines deployed is directly affected by the amount of funding and available resources, and is a function of TSA's risk-based analysis of how best to distribute technology across all airports to maximize passenger safety.

20. As set forth in the Screening Checkpoint SOP, where an

AIT machine has not yet been deployed to a particular airport or screening checkpoint, walk-through metal detectors are the primary screening method, along with other alternative and supplemental screening methods as needed.

21. When TSA deploys an AIT machine, signage is used to inform the public that the machine may be used as part of their screening process. This signage, which includes examples of the pictures that the machine generates, is frequently located at the point where passengers' identification and boarding passes are checked, but may be located closer to the AIT machine as the configuration of TSA's checkpoints and positioning of the AIT machines varies widely. The notice also advises the individual that they may decline AIT screening and be screened by a pat-down instead. The AIT screening is conducted at the checkpoint, which is a heavily trafficked public area, by trained TSOs, and lasts less than fifteen seconds.

Pat-Down Procedures

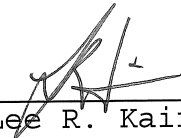
22. As set forth in the Screening Checkpoint SOP, if a passenger chooses to opt out of screening via an AIT machine, or sets off an alarm of one of the AIT machines or a walk-through metal detector, or is unable to proceed through either the AIT or the walk-through metal detector due to a medical condition or physical constraint, or requests private screening, that passenger will undergo a pat-down. While only a small

percentage of passengers ultimately receive pat-downs, this procedure helps TSA find possible explosives, chemical weapons, and other dangerous items that otherwise might go undetected. If a passenger goes through AIT and does not alarm, that person would not be subject to a pat-down with the exception of a very small percentage of pat-downs that are performed at random so that TSA can use unpredictability as a further deterrent to terrorists.

23. The pat-down procedures were revised by the Screening Checkpoint SOP because, based upon TSA's expertise, daily intelligence reports, and the results of repeated covert testing, TSA concluded that it needed to enhance its pat-down procedures, which are now more consistent with standard practices at other airports around the world. The pat-down procedures also needed to be able to detect non-metallic threat items in sensitive areas equally as well as AIT to prevent a security vulnerability by allowing passengers to opt out of AIT. Therefore, TSA adjusted the standard pat-down policy to use techniques that are informed by the latest intelligence, included but not limited to the attempt by Mr. Abdulmutallab to blow up an American airplane over the United States on December 25, 2009, using a non-metallic explosive device that was concealed in a sensitive area.

Pursuant to 28 U.S.C. § 1746, I declare under penalty of perjury that the foregoing is true and correct.

Dated: March 30, 2011.



Lee R. Kair
Assistant Administrator For Security
Operations
Transportation Security Administration
Department of Homeland Security